Several Fault Attacks on Smart Card Signature Schemes

Priyam Biswas (MSECE), Brian King
prbiswas@iupui.edu
Department of Electrical and Computer Engineering, Indiana University-Purdue University Indianapolis, USA

Today's financial industry is moving towards digital signature enabled applications using smart card technology. Worldwide, many financial organizations have mandated to use smart card for financial credit and debit transfer. In addition, the United States government has adopted smart card technology for its major credentialing initiatives. So, a small security flaw can cost a massive loss in the industry, hence the security measurements of smart card is immense. A variety of attacks on smart card enabled signatures schemes have been proposed. In this work we discuss several fault attacks. Here, the attacker induces a fault on the smart card during the signature generation process as executed on the smart-card, thus outputting a faulty signature. By repeating this attack several times, the attacker collects enough faulty outputs that they can calculate the signing key. With this key, the attacker is then free to conduct transactions without any financial repercussion. In this work we discuss three types of fault attacks, the bit-flip attack, the counter fault attack and the doubling attack. Apart from implementing these attacks, the main challenge is to identify the valid patterns that can be used to match the correct key bits. Pruning invalid patterns (patterns that produce "false positive results") also plays a significant role as it effectively reduces the time required for matching. We address this issue by constructing state machines which efficiently provide possible valid patterns and the algorithms that can be used to calculate the signing key.

References:

[1] Ling, Jie, and Brian King. "Smart card fault attacks on elliptic curve cryptography." In Circuits and Systems(MWSCAS), 2013 IEEE 56th International Midwest Symposium on, pp. 1255-1258. IEEE, 2013.

[2]http://www.library.ca.gov/crb/rfidap/docs/SCA-Smart_Cards_and_Logical_Access_Report.pdf Accessed on 23 March, 2015.